IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF VIRGINIA

RICHMOND DIVISION

Trinity Bias, Jaime Cardenas, Christopher Holmes and Robert Shaw, individually and on behalf of all others similarly situated, Plaintiffs, v. Elephant Insurance Company, Elephant Insurance Services, LLC, and Platinum General Agency, Inc. d/b/a Apparent Insurance, Defendants.	Civil Action No. 3:22-cv-00487-JAG **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Trinity Bias, Jaime Cardenas, Christopher Holmes and Robert Shaw, individually, and on behalf of all others similarly situated ("Plaintiffs"), upon personal knowledge of facts pertaining to them and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Consolidated Class Action Complaint against Defendants Elephant Insurance Company; Elephant Insurance Services, LLC; and Platinum General Agency, Inc. d/b/a Apparent Insurance (collectively "Elephant" or "Defendants"), and allege as follows:

I. INTRODUCTION

1. Every year millions of Americans have their most valuable personal information stolen and sold online because of data breaches and unauthorized data disclosures. Despite warnings about the severe impact of unauthorized data disclosures on Americans of all economic strata, companies—including Defendants—still fail to put adequate security measures in place to prevent the unauthorized disclosure of private data belonging to their customers or potential

customers. This action arises out of the recent data breach at Elephant, an automobile insurance provider, that targeted the sensitive information of Plaintiffs and Class Members in Elephant's possession, custody or control.

2. In the past two years, industry experts have specifically highlighted the importance of driver's license numbers and the ways in which a coordinated campaign by hackers and malicious attackers is dedicated to collecting those numbers to commit identity theft. In fact, a driver's license is a critical part of a fraudulent, synthetic identity that can be sold on the dark web and is a jackpot for thieves that can be used to create fake driver's licenses or other fake IDs, open fraudulent accounts, avoid traffic tickets or collect government benefits such as unemployment checks, and use for verification on any government form that requires identity verification. Driver's license numbers are also exceptionally useful for fraudsters to craft curated phishing attacks and impersonate government officials to obtain even more information or insert malicious links or attachments into email.

3. Drivers' license numbers have been taken from auto-insurance providers by hackers in multiple other attacks, including Geico, Farmers, USAA, Kemper, Metromile, and American Family—all in 2021—indicating this particular form of personal information is in high demand and that sophisticated insurance companies like Defendants knew or had reason to know their security practices were of particular importance to safeguard consumer data. This is especially true given that the New York State Department of Financial Services ("NYSDFS") issued an insurance industry letter on February 16, 2021, stating it recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal the exact

kind of information stolen here, and to flag that such information was being used to submit fraudulent claims for pandemic and unemployment benefits."[1]

4. Defendants provide automobile insurance to customers in multiple states throughout the country. Defendants claim they "are committed to protecting your privacy by maintaining and using your personal information responsibly."[2] And Defendants promise to "disclose your personal information only as permitted by law."[3] They further promise:

> We restrict access to your personal information to our employees and others who we determine must use it to provide our products and services or otherwise have a business need to know the information. We require those individuals with access to your personal information to protect it and keep it confidential. Their use of the information is limited by law, our employee Code of Ethics, and written agreements when appropriate. We also maintain physical, electronic, and procedural safeguards that comply with applicable legal requirements to protect your information.[4]

5. Yet, Defendants intentionally configured and designed their online insurance quoting platform to generate responses to requests for insurance quotes that included personal information ("PI") from motor vehicle records that was auto-populated and obtained from third-party data providers. The disclosure of PI, including driver's license numbers, was provided to anyone who submitted a request, regardless of whether those requests were submitted by individuals actually seeking a quote or not. If not for Defendants' intentional and knowing configuration and design of its systems, Plaintiffs' and Class Members' PI would not have been disclosed to cyber criminals.

---

[1] Industry Letter, New York Department of Financial Services Industry Letter (February 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert (last accessed Sept. 14, 2022).

[2] *Elephant Insurance Privacy Notice*, Elephant Insurance, available at: https://www.elephant.com/privacy (last accessed Sept. 14, 2022).

[3] *Id.*

[4] *Id.*

6. Defendants failed to meet their promises and obligation to protect the sensitive personal information they collected, maintained, and used. Despite knowing that driver's license information is highly sensitive and legally restricted as a result of the Driver's Privacy Protection Act ("DPPA"), 18 U.S.C. § 2724, Defendants failed to secure this highly sensitive information collected from Departments of Motor Vehicles, applications, customers, data aggregators, and their online insurance quoting platform, thereby making it public without consent and in violation of their own corporate promises and policy.

Unauthorized Data Disclosure

7. Between at least March 26, 2022 through April 1, 2022—as reported by Elephant to the public on May 6, 2022 and to regulators starting May 26, 2022—Defendants believe "certain consumer information may have been viewed on or copied from Elephant Insurance's network," including the following sensitive information from Plaintiffs and Class Members: "name, driver's license number, and date of birth."[5] In statements to regulators, Defendants estimated at least 2,762,687 individuals were affected and notified,[6] including Plaintiffs. Elephant also states it discovered the breach on April 25, 2022,[7] identified the affected individuals and data that same day,[8] and yet waited two weeks to issue a statement and more than a month to provide actual notice to affected individuals.

8. Defendants are legally required to protect the personal information they gather from exfiltration and unauthorized access. PI is defined as including a person's Social Security number,

---

[5] *Elephant Insurance Provides Notice of Data Event*, PR NewsWire (May 6, 2022), available at: https://www.prnewswire.com/news-releases/elephant-insurance-provides-notice-of-data-event-301542026.html (last accessed Sept. 14, 2022).

[6] Office of the Maine Attorney General, Data Breach Notifications (May 26, 2022), available at: https://apps.web.maine.gov/online/aeviewer/ME/40/604c3805-9ac9-4bcc-938b-813905d66182.shtml (last accessed Sept. 14, 2022).

[7] *Id.*

[8] *Elephant Insurance Provides Notice of Data Event*, *supra* note 5.

driver's license number, name, address, telephone number, and medical or disability information.[9] Defendants acknowledge this in their privacy policy when they characterize the information they collect, including driver's license numbers and dates of birth, as "Nonpublic Personal Information."[10]

9. As a result of Defendants' failure to provide reasonable and adequate data security, including their intentionally configured and designed online insurance quoting platform, Defendants violated state and federal law by improperly disclosing Plaintiffs' and the Class Members' PI—including their especially sensitive driver's license information obtained from motor vehicle records— to unauthorized parties and/or entities. As a direct result of Defendants' acts and/or omissions, including their failure to follow basic security procedures, such as validating the identity of insurance applicants before disclosing their highly sensitive PI, unauthorized parties are already attempting to use the improperly disclosed information to commit identity theft and fraudulently open financial accounts in Plaintiffs' names. Plaintiff Cardenas has already determined that his driver's license is available on the dark web.

10. Plaintiffs and Class Members are now at much higher risk of continued identity theft and for cybercrimes of all kinds, especially considering the highly valuable and sought-after private PI stolen here, and have suffered damages related to lost time, loss of privacy, and other harms.

[9] 18 U.S.C. § 2725(3).
[10] *See Elephant Insurance Privacy Notice, supra* note 2.

II. PARTIES

Plaintiffs

11. Jaime Cardenas is a resident of Blanco, Texas. On or about June 7, 2022, Plaintiff Cardenas received notice via email from Defendants that they improperly exposed his PI to unauthorized third parties.

12. Trinity Bias is a resident of Joliet, Illinois. On or about May 26, 2022, Plaintiff Bias received notice via mail dated May 23, 2022, from Defendants that they improperly exposed her PI to unauthorized third parties.

13. Christopher Holmes is a resident of Big Springs, Texas. Plaintiff Holmes received notice via mail dated June 3, 2022, from Defendants that they improperly exposed his PI to unauthorized third parties.

14. Robert Shaw is a resident of Galena, Kansas. Plaintiff Shaw received notice via a letter dated May 23, 2022, from Defendants that they improperly exposed his PI to unauthorized third parties.

Defendants

15. Elephant Insurance Company is a Virginia Stock Corporation with its principal place of business located in Henrico, Virginia. Elephant Insurance Company is licensed to do business and markets, sells, and underwrites automobile insurance policies in Georgia, Illinois, Indiana, Maryland, Ohio, Tennessee, Texas, and Virginia. Elephant Insurance Company is a wholly-owned subsidiary of Admiral Group, plc., a U.K. insurer.[11]

16. Elephant Insurance Services, LLC, is a privately held insurance company organized under the laws of the state of Delaware and a principal place of business in Henrico, Virginia.

[11] *About Elephant*, Elephant Insurance, https://www.elephant.com/about (last accessed Sept. 14, 2022) "Elephant is a subsidiary of Admiral Group plc."

Elephant Insurance Services, LLC, is licensed to do business and markets and sells automobile, homeowners, renters, motorcycle, and life insurance policies in Georgia, Illinois, Indiana, Maryland, Ohio, Tennessee, Texas, and Virginia.

17. Platinum General Agency, Inc., d/b/a Apparent Insurance is a corporation organized under the laws of the State of Texas, with its principal place of business in Henrico, Virginia. Apparent Insurance is licensed to do business and markets and sells automobile, homeowners, renters, motorcycle, and life insurance policies in Georgia, Illinois, Indiana, Maryland, Ohio, Tennessee, Texas, and Virginia. Defendant Platinum General Agency, Inc. is, upon information and belief, a wholly owned subsidiary of Elephant Insurance Company, and utilizes "Apparent Insurance" as a trade name.[12]

III. JURISDICTION AND VENUE

18. Subject matter jurisdiction in this civil action is authorized pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendants, and the amount in controversy exceeds $5 million, exclusive of interest and costs. The Court also has federal question jurisdiction under 28 U.S.C. § 1331 for the Drivers' Privacy Protection Act claims and supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

19. This Court has personal jurisdiction over Defendants because they maintain their principal place of business in this District, are authorized to and regularly conduct business in this District and in the Commonwealth of Virginia, and have sufficient minimum contacts with the

[12] *About Us—Our Extended Family*, Apparent Insurance, https://www.apparentinsurance.com/about-us/extended-family/ (last accessed Sept. 14, 2022), listing Admiral Group plc as the parent company, and Apparent Insurance as a brand of Platinum General Agency, Inc.

Commonwealth of Virginia. Defendants make decisions regarding the corporate governance and management of their insurance business, including decisions regarding the security measures to protect its customers' PI, in this District. Defendants also intentionally avail themselves of this jurisdiction by promoting, selling, and marketing their services from Virginia to millions of consumers nationwide.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a) through (d) because Defendants reside in this District and, on information and belief, a substantial part of the events or omissions giving rise to Plaintiffs' and Class Members' claims emanated from this District, including, without limitation, decisions made by Defendants' governance and management personnel or inaction by those individuals that led to misrepresentations, invasions of privacy, and the Unauthorized Data Disclosure.

21. Venue is proper in this division of the District pursuant to Eastern District of Virginia Local Civil Rule 3(B)(4) and 3(C) because Defendants Elephant Insurance Services, LLC, and Elephant Insurance Company are headquartered and reside in the Richmond Division.

IV. FACTUAL ALLEGATIONS

A. Defendants Collect PI but Failed to Adhere to Non-Disclosure Requirements and Promises.

22. Elephant is a "customer-centric direct insurer headquartered in Henrico, Virginia" that was founded in 2009.[13] Elephant sells automobile, homeowners, renters, motorcycle, and life insurance policies as the subsidiary of a UK insurance company with a presence in eight countries with six million worldwide customers. "Elephant may not seem like the most logical name for an insurance company, but actually, it's a pretty great fit. We think the qualities of an elephant perfectly match how we do business and approach insurance. Elephants are big, strong, and built

[13] *About Elephant*, *supra* note 10.

to last. At the same time, they are kind, caring, and look out for their herd." Elephant sells itself as "big enough to matter but small enough to care."

23. Like other insurance providers, Elephant collects various kinds of PI, including information from motor vehicle records, through multiple processes: online applications through a quote website, other application processes, consumer report information, Departments of Motor Vehicles, transaction information, and website information.[14] Defendants specifically acknowledge and designate this information as "Nonpublic Personal Information."

24. The "Nonpublic Personal Information" collected and stored by Defendants is substantially wider in scope than what Elephant reports was accessed and exfiltrated from its network and includes: name, street address, phone number, e-mail address, driver's license number, Social Security Number, date of birth, gender, marital status, vehicle information, information about other drivers using a vehicle, driving record, insurance policy information, claims history with Defendants and with other insurers, credit report information, financial information such as billing and payment information, and website information such as the website that linked customers to Elephant, the computer operating system used, site pages visited, and "cookies" stored on the user computer, which collect technical data such as an Internet Protocol (IP) address, operating system, and session ID.[15]

25. In April 2022, Defendants "identified unusual activity in our network."[16] After an investigation, Elephant determined that information including names, driver's license information, and addresses may have been "viewed on or copied from our network." Elephant has not provided

[14] *See Elephant Insurance Privacy Notice, supra* note 2.
[15] *Id.*
[16] *Notice of Data Event*, Elephant Insurance, https://www.elephant.com/notice-of-data-event (last accessed July 5, 2022), also available at http://web.archive.org/web/20220509164301/https://www.elephant.com/notice-of-data-event (last accessed Sept. 14, 2022).

additional details on the mechanism through which the incident occurred, how Elephant limited the information accessed and exfiltrated to only a subset of the PI it collects, or how Elephant determined which individuals to notify. This incident is referred to herein as the "Unauthorized Data Disclosure."

26. Plaintiffs Cardenas, Bias, Holmes and Shaw, along with other members of the Class, received a letter from Elephant titled "Notice of Data Incident." Plaintiff Cardenas' notification was dated June 7, 2022; Plaintiff Bias's notification was dated May 23, 2022; Plaintiff Holmes's notification was dated June 3, 2022 and Plaintiff Shaw's notification was dated May 23, 2022. The letters stated that their PI, detailed below, may have been compromised, and included the following:

> **Notice of Data Incident**
>
> Elephant Insurance, and our subsidiary Apparent Insurance (together, "Elephant Insurance"), value and respect the privacy of your information which is why we are writing to let you know about a recent incident that may involve some of your information. We have your information because you either are a current or previous Elephant Insurance customer or we received your information as part of providing a quote for auto or other insurance coverage. This letter provides you with information about the incident, our response, and resources available to you.
>
> **What Happened?** In April 2022, we identified unusual activity on our network. We promptly undertook a comprehensive investigation, working with third-party specialists, to secure our systems and to confirm the nature and scope of the incident, as well as any impact to information on our network. Through the investigation, we determined that certain consumer information may have been viewed on or copied from our network between March 26, 2022 and April 1, 2022. We undertook a comprehensive review to determine what information was impacted and to whom it related. You are receiving this letter because, on April 25, 2022, our review determined that your information was in the affected data.
>
> **What Information Was Involved?** Our investigation determined that the affected information includes your name and driver's license number.
>
> **What We Are Doing.** Upon identifying unusual system activity, we took prompt measures to secure our systems, investigate this incident, and determine what information may be affected. We reported the incident to federal law enforcement and are notifying appropriate state regulatory agencies. As part of our ongoing

> commitment to information security, we are also reviewing and enhancing our existing safeguards and procedures.
>
> As an added precaution, we are offering you access to 12 months of credit monitoring services at no cost to you. To activate these services, please follow the instructions included in the attached ***Steps You Can Take to Help Protect Information***.
>
> **What You Can Do**. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You should promptly report any activity indicative of identity theft or fraud immediately to law enforcement. Please also review the information contained in the attached ***Steps You Can Take to Help Protect Information***.
>
> **For More Information**. We understand that you may have questions that are not addressed in this notice. If you have additional questions, please call our dedicated assistance line at (855) 788-2603, which is available from 9:00 AM to 6:30 PM EST Monday through Friday (excluding major U.S. holidays).
>
> Sincerely,
>
> Elephant Insurance Services, LLC
>
> www.elephant.com[17]

27. The Notice confirms Plaintiffs were victims of the Unauthorized Data Disclosure and that Defendants obtained their sensitive PI "because you either are a current or previous Elephant Insurance customer or we received your information as part of providing a quote for auto or other insurance coverage." The Notice also confirms that driver's license numbers were acquired, and that Elephant has reason to believe they may have been "viewed on or copied from" Defendants' servers.

28. After receiving Unauthorized Data Disclosure notice letters, Plaintiffs and Class Members now face a substantial present and increased risk of fraud and identity theft), and that

[17] *Notice of Data Breach*, as filed with the California Attorney General, https://oag.ca.gov/ecrime/databreach/reports/sb24-553749 and https://oag.ca.gov/system/files/Elephant%20Insurance%20Sample%20Notice.pdf (last accessed on Sept. 14, 2022).

they must take steps to mitigate that risk of harm. In fact, Defendants' letter specifically instructs Plaintiffs and the Class to take mitigative their losses: "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You should promptly report any activity indicative of identity theft or fraud immediately to law enforcement."[18] This is because the drivers' license numbers are taken for the purpose of committing fraud in the name of the person whose license information is taken.

B. <u>The PI Disclosed by Defendants as a Result of Their Disregard for Basic Data Security is Highly Valuable on the Black Market.</u>

29. The information Defendants failed to protect in violation of state and federal law is very valuable to phishers, hackers, identity thieves, and cyber criminals, especially at this time where unprecedented numbers of criminals are filing fraudulent unemployment benefit claims and driver's license information is uniquely connected to financial fraud, as well as to the ability to file a fraudulent unemployment benefit claim.

30. Indeed, hackers often aggregate information taken from data breaches on users to build profiles on individuals. These profiles combine publicly available information with information discovered in previous data breaches and exploited vulnerabilities. There are few data breaches that provide a comprehensive snapshot of any one individual person. Unique and persistent identifiers such as Social Security Numbers, driver's license numbers, usernames, and financial account numbers (e.g., credit cards, insurance policy numbers, etc.) are critical to easily forging an identity. When not all information is available, the stolen information is used to socially engineer a victim into providing additional information so a "fullz"[19] profile can be obtained.

---

[18] *Id.*

[19] "Fullz" is slang used by threat actors and various criminals meaning "full information," a complete identity profile or set of information on any entity or individual.

31. For example, a health care system and a retail store point-of-sale system may have two unrelated data breaches where an individual's information is taken. The individual's driver's license may not be in either of those data bases, but after the Unauthorized Data Disclosure, a threat actor could have improved the profile and added a driver's license number. The value of that profile would allow such crimes as identity theft, financial crimes, and even illegal voting that would not previously have been possible.

32. There is no legitimate or legal reason for anyone to use Defendants' inadequate website security to acquire driver's license information of Plaintiffs and the Class. The only reason is for immediate or eventual malicious intent, since no one would go to the trouble of obtaining data that had no value. Any non-public data, especially government issued identification numbers like a driver's license or non-driver's identification number, has criminal value. On the darknet markets, a driver's license, combined with the full name and state issued, is a sought-after data point. Darknet markets are a downstream "flea market" for data to be sold, usually not by the original threat actor or criminal group. It is a dumping ground, usually after the data has been exploited.

33. The value of stolen driver's license information currently has a darknet market ("DNM") value of $1 per license. This was re-verified on March 3, 2022, accessing several DNMs using a trusted identity. Social Security Numbers, once considered the "gold standard" of identity fraud, are also selling for $1 per value in those same markets. This illustrates the value of driver's license information to cybercriminals and people committing identity fraud. According to popular darknet markets, cyber criminals value driver's licenses equally to Social Security Numbers.

34. In some ways, driver's license numbers are even more attractive than Social Security Numbers to threat actors and more dangerous to the consumer when compromised. Unlike

a Social Security Number, a driver's license number is not monitored as closely, so it can potentially be used in ways that will not immediately alert the victim. Threat actors know this as well. Because driver's licenses contain, or can be used to gain access to, uniquely qualifying and comprehensive identifying information such as eye color, height, weight, sex, home address, medical or visual restrictions, and living will/health care directives, most insurance and credit agencies highly recommend that immediate notice, replacement, and identity theft protections are put in place for a minimum of three years. Most cyber experts, including Enterprise Knowledge Partners, recommend five years or more.

35. Stolen driver's licenses can be used (alone or in combination with other information) by malicious actors to accomplish the following:

- Apply for credit cards;
- Apply for financial loans (especially student loans);
- Open bank accounts;
- Obtain or create fake driver's licenses;
- Given to police for tickets;
- Provided to accident victims;
- Collect government unemployment benefits;
- Create and sell underage fake IDs;
- Replace/access account information on:
    - LinkedIn,
    - Facebook/Meta,
    - WhatsApp,
    - Instagram;

- Obtain a mobile phone;
- Dispute or prove a SIM swap;
- Redirect U.S. mail;
- Apply for unemployment benefits;
- Undocumented individuals may use them as a method to gain access to the U.S., and claim a lost or stolen passport;
- Create a fake license as a baseline to obtain a Commercial Driver's License;
- File tax returns or gain access to filed tax returns; and
- Engage in phishing and other social engineering scams.

36. Unsecured sites that contain or transmit PI, such as a driver's license, require notice to consumers when the data is stolen because it can be used to perform identity theft and other types of fraud. A threat actor is usually motivated by financial or political gain before it exerts time, and skill to compromise and exfiltrate. Over time, identity thieves have systematized their criminal activities to gather important pieces of a synthetic identity from multiple breaches and sources. The theft of a driver's license number is no less valuable in that endeavor than the theft of a Social Security Number, as demonstrated by these two unique identifiers carrying the same price on the darknet, and by the fact that the identity thieves have demonstrated a systematic and businesslike process for collecting these stolen driver's license numbers in this Unauthorized Data Disclosure and others committed against insurers.

37. The frequency of cyberattacks has increased significantly in recent years.[20] In fact, "Cyberattacks rank as the fastest growing crime in the US, causing catastrophic business disruption. Globally, cybercrime damages are expected to reach US $6 trillion by 2021."[21]

38. Cybersecurity Ventures, a leading researcher on cybersecurity issues,

> expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a year, and will be more profitable than the global trade of all major illegal drugs combined.[22]

39. As noted in recent reports by Deloitte and Interpol, cyberattacks have greatly increased in the wake of the COVID-19 pandemic.[23]

40. As alleged above, stolen PI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

---

[20] *See The Cost of Cybercrime,* Accenture Security (2019), https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf (last accessed Sept. 14, 2022).

[21] *Top Cyberattacks of 2020 and How to Build Cyberresiliency*, ISAC (Updated Feb. 3, 2021), https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency (last accessed Sept. 14, 2022) (citing Cybersecurity Ventures, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016).

[22] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2020*, Cybercrime Magazine (Nov. 13, 2020), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (last accessed Sept. 14, 2022).

[23] Cedric Nabe, *Impact of COVID-19 on Cybersecurity*, Deloitte, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (last accessed Sept. 14, 2022); Interpol, *Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception*, https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (last accessed Sept. 14, 2022).

41. When malicious actors infiltrate companies and exfiltrate the PI that those companies store or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[24] "Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015).

42. Consumers' PI remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[25] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[26] Alternatively, criminals are able to purchase access to entire company data breaches for $900 to $4,500.[27] (Note: the prices can vary depending on the point in the chain – verified identities may sell for higher prices early in the chain, then for the lower prices described above when they reach the "flea market sites.")

43. The information compromised in the Unauthorized Data Disclosure is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. And the information

---

[24] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce (Feb. 2, 2020), https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last accessed Sept. 14, 2022).

[25] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Sept. 14, 2022).

[26] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Sept. 14, 2022).

[27] *In the Dark*, VPNOverview, 2019, *available at* https://tinyurl.com/mr3nsc24 (last accessed Sept. 14, 2022).

compromised in the Unauthorized Data Disclosure can be used to *open* fraudulent bank accounts and credit and debit cards, as well as benefits accounts in various state benefits offices, compounding the identity theft and cycle of black market sales detailed above. The driver's license numbers compromised in this Unauthorized Data Disclosure are also more valuable because driver's license numbers are long lasting, and difficult and problematic to change.

44. Recently, Forbes writer Lee Mathews reported on Geico's unauthorized data disclosure that included driver's license numbers:

> Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200.[28]

45. National credit reporting company, Experian, blogger Gayle Sato also emphasized the value of driver's license information to thieves and cautioned:

> Your driver's license may not seem like a jackpot for thieves, but it can be used to create fake driver's licenses, open accounts in your name, avoid traffic tickets or collect government benefits such as unemployment checks. Worse, if your license data has been stolen in a data breach, you may not even know it's being misused.[29]

46. In fact, according to CPO Magazine, which specializes in news, insights, and resources for data protection, privacy, and cyber security professionals,

> To those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: " . . . It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may

[28] Lee Mathews, *Hackers Stole Customers' License Numbers from Geico in Months-Long Breach*, Forbes (April 20, 2021), https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658 (last accessed Sept. 14, 2022).

[29] Gayle Sato, *What Should I Do If My Driver's License Number Is Stolen?* (Nov. 3, 2021), https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last accessed Sept. 14, 2022).

> be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email.[30]

47. Drivers' license numbers have been taken from auto-insurance providers by hackers in other circumstances, including Geico, Farmers, USAA, Kemper, Metromile, and American Family all in 2021, indicating both that this particular form of PI is in high demand[31] and also that Defendants knew or had reason to know that their security practices were of particular importance to safeguard consumer data.[32]

48. In fact, when Geico announced that its online quoting platform was subject to a breach, its data breach notice filed with the California Attorney General explicitly stated that GEICO had "reason to believe that this information could be used to fraudulently apply for unemployment benefits in your name."[33]

---

[30] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO Magazine (April 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed Sept. 14, 2022).

[31] *Id.*

[32] *See* United States Securities and Exchange Commission Form 8-K for INSU Acquisition Corp. II (Feb. 1, 2021), https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?=1819035-01022021 (last accessed Sept. 14, 2022) (announcing a merger with auto-insurance company MetroMile, Inc., an auto-insurer, which announced a drivers' license number Data Disclosure on January 19, 2021); Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021), https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed Sept. 14, 2022) (describing a scam involving drivers' license numbers and Progressive Insurance).

[33] *See GEICO Notice of Data Breach, https://www.documentcloud.org/documents/20618953-geico-data-breach-notice* (last accessed Sept. 14, 2022), (notice filed with Calif. Attorney General dated April 9, 2021).

49. Further, an article on TechCrunch explains that it is driver's license or non-driver's identification numbers themselves that are the critical missing link for a fraudulent unemployment benefits application: "Many financially driven criminals target government agencies using stolen identities or data. But many U.S. states require a government ID — like a driver's license — to file for unemployment benefits. To get a driver's license number, fraudsters take public or previously breached data and exploit weaknesses in auto insurance websites to obtain a customer's driver's license number. That allows the fraudsters to obtain unemployment benefits in another person's name."[34]

50. For example, the New York State Department of Financial Services issued an industry letter on February 16, 2021, stating that they had "recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal [NPI, including] websites that provide an instant quote. . . . [I]t received reports from two auto insurers in late December 2020 and early January 2021, that cybercriminals were targeting their websites that offer instant [] quotes [] to steal unredacted driver's license numbers. . . . . DFS has confirmed that, at least in some cases, this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits . . . DFS [] has also discovered communications on cybercrime forums offering to sell techniques to access driver's license numbers from auto insurance websites and step-by-step instructions on how to steal them."[35]

51. Once PI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details, or to fraudulently

[34] Zach Whittaker, *Geico Admits Fraudsters Stole Customers' Driver's License Numbers for Months*, TechCrunch (Apr. 19, 2021), https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/#:~:text=To%20get%20a%20driver's%20license,benefits%20in%20another%20person's%20name (last accessed Sept. 14, 2022).

[35] Industry Letter, *supra* note 1.

manufacture new accounts for access and sale. This can lead to additional PI being harvested from the victim, as well as PI from family, friends and colleagues of the original victim.

52. Victims of drivers' license number theft also often suffer unemployment benefit fraud, harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts. Unauthorized data disclosures facilitate identity theft as hackers obtain consumers' PI and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PI to others who do the same.

53. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PI to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[36] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[37]

C. Defendants Were on Notice of the Sensitive and Private Nature of the PI they Stored and Utilized for Insurance Quotes, and Their Duty to Safeguard the PI.

54. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PI and of the foreseeable consequences if their data security systems were breached, including the significant costs that would be imposed on Plaintiffs and the Class as a result of a breach.

[36] *See Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown,* Government Accountability Office (June 2007), http://www.gao.gov/assets/270/262899.pdf (last accessed Sept. 14, 2022).
[37] *Id.*

55. Defendants knowingly refrained from implementing basic security measures to protect Plaintiffs' and Class Members' PI, including information obtained from motor vehicle records, in spite of having control over the configuration and design of their online quoting platform.

56. In fact, NYSDFS, in their February 16, 2021, industry letter recommended the following steps for entities that maintain public-facing websites:

a. Conduct a thorough review of public-facing website security controls, including but not limited to a review of its Secure Sockets Layer (SSL), Transport Layer Security (TLS), and HTTP Strict Transport Security (HSTS and Hypertext Markup Language (HTML) configurations.

b. Review public-facing websites for browser web developer tool functionality. Verify and, if possible, limit the access that users may have to adjust, deface, or manipulate website content using web developer tools on the public-facing websites.

c. Review and confirm that its redaction and data obfuscation solution for NPI is implemented properly throughout the entire transmission of the NPI until it reaches the public-facing website.

d. Ensure that privacy protections are up to date and effectively protect NPI by reviewing who is authorized to see NPI, which applications use NPI, and where NPI resides.

e. Search and scrub public code repositories for proprietary code.

f. Block the IP addresses of the suspected unauthorized users and consider a quote limit per user session.[38]

57. Due to the "ongoing cybercrime campaign that is a serious threat to consumers," NYSDFS issued a Cyber Fraud Alert Follow-up on March 30, 2021. They urged "**personal lines insurers and other financial services companies to avoid displaying prefilled NPI on public facing websites considering the serious risk of theft and consumer harm**. (Emphasis in

[38] Industry Letter, *supra* note 1. Note that this Industry Letter was reported online on numerous websites, including: https://digitalguardian.com/blog/public-facing-financial-services-sites-ripe-data-theft (Feb. 23, 2021); and https://www.gravoc.com/2021/04/09/cyber-fraud-alert-issued-for-websites-collecting-npi/ (Apr. 9, 2021) (last accessed Sept. 14, 2022).

original). We note that many of the auto insurers targeted by this cybercrime campaign have recently disabled all NPI prefill on their public-facing websites."[39]

58. NYSDFS also recommended that "[t]o combat this cybercrime, the following basic security steps should be implemented…

a. Disable prefill of redacted NPI. Avoid displaying prefilled NPI, especially on public facing websites.

b. Install Web Application Firewall (WAF). WAFs help protect websites from malicious attacks and exploitation of vulnerabilities by inspecting incoming traffic for suspicious activity.

c. Implement CAPTCHA. Cybercriminals use automated programs or "bots" to steal data. Completely Automated Public Turing Tests ("CAPTCHA") attempt to detect and block bots.

d. Improve Access Controls for Agent Portals. Agent portals typically allow agents access to consumer NPI, and robust access controls are required by DFS's cybersecurity regulation.

e. Training and awareness. Employees and agents should be trained to identify social engineering attacks. Employees and agents should know not to disclose NPI, including DLNs, over the phone. Robotic scripts with grammatical errors or repeated statements used during dialogue are key identifiers of fraudulent calls.

f. Limit access to NPI. Employees and agents should only have access to sensitive information that is necessary to do their job.

g. Wait until payments have cleared before issuing a policy. Auto insurers should consider waiting until an eCheck, credit card, or debit card payment has been cleared by the issuing bank before generating an online policy and granting the policyholder access to NPI.

h. Protect NPI received from data vendors. Ensure that APIs used to pull data files, including JSON and XML, from data vendors are not directly accessible for the internet or agent portals.[40]

[39] Industry Letter, New York Department of Financial Services Industry Letter (March 30, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210330_cyber_alert_followup, (last accessed Sept. 14, 2022).

[40] *Id.*

59. "Insurance companies are desirable targets for cyber attackers because they work with sensitive data."[41] In fact, according to the Verizon 2020 Data Breach Investigations Report, there were 448 confirmed data breaches in the financial and insurance industries.[42] That increased to 690 confirmed data breaches in the 2022 report.[43]

60. In 2021, drivers' license numbers were taken from auto-insurance providers by hackers in multiple attacks on similar companies, including Geico, Farmers, USAA, Kemper, Metromile, and American Family. This proves this particular form of personal information is in high demand by hackers and also that sophisticated insurance companies like Defendants knew or were on notice that their security practices were of particular importance to safeguard consumer data.

61. Defendants claim they "are committed to protecting your privacy by maintaining and using your personal information responsibly."[44] And Defendants promise to "disclose your personal information only as permitted by law."[45] Defendants further promise:

> We restrict access to your personal information to our employees and others who we determine must use it to provide our products and services or otherwise have a business need to know the information. We require those individuals with access to your personal information to protect it and keep it confidential. Their use of the information is limited by law, our employee Code of Ethics, and written agreements when appropriate. We also maintain physical, electronic, and procedural safeguards that comply with applicable legal requirements to protect your information.[46]

---

[41] Data Protection Compliance for the Insurance Industry, Ekran System (October 7, 2020), https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry (last accessed Sept. 14, 2022).

[42] 2020 Data Breach Investigations Report, Verizon, https://www.verizon.com/business/resources/reports/2020-data-breach-investigations-report.pdf (last accessed Sept. 14, 2022).

[43] 2022 Data Breach Investigations Report, Verizon, https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf (last accessed Sept. 14, 2022).

[44] *Elephant Insurance Privacy Notice, supra* note 2.

[45] *Id.*

[46] *Id.*

62. In addition, Elephant is an insurance company that sells auto insurance and uses motor vehicle records to verify identities and underwrite policies. Their underwriting and other insurance activities are explicitly subject to the DPPA, which was enacted in 1994 and has been in effect for almost two decades. During Defendants' entire time of existence as an insurer in the United States—since it was founded in 2009—insurance activities and PI regulation have been subject to the DPPA.

63. Furthermore, Defendants consciously use PI, including driver's license numbers and other motor vehicle records stored on or accessed by their systems that they intentionally disclose when generating insurance quotes. Defendants' continual collection of PI in the form of customer information, driving records, accident reports, and other motor vehicle information, along with their insurance underwriting and business collection of driver's license and other motor vehicle information, put Elephant in the position of knowing that it was obligated to protect the privacy of customers and potential customers like Plaintiffs and members of the class.

64. As a result, Defendants' safety and security promises were facially insufficient. Despite the clear danger that insecure use of PI poses, Defendants knowingly chose to configure and design their online quoting system in a manner which allowed access to and disclosure of Plaintiffs' and Class Members' driver's license numbers, which are motor vehicle records, in violation of Defendants' company policy and applicable law.

D. Defendants Failed to Comply with Federal Trade Commission Requirements.

65. Federal and state governments established security standards and issued recommendations to minimize unauthorized data disclosures, and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses highlighting the importance of implementing reasonable data security

practices. According to the FTC, the need for data security should be factored into all business decision-making.[47]

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[48] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[49]

67. The FTC recommends that companies not maintain PI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[50]

68. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, treating the failure to employ reasonable and appropriate measures to

[47] *Start With Security: A Guide for Business*, Federal Trade Commission (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Sept. 14, 2022).

[48] *See Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Sept. 14, 2022).

[49] *Id.*

[50] *See Start With Security, supra* note 47; *Protecting Personal Information, supra* note 48.

protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[51]

69. Failing to take basic security measures in designing and implementing their computer systems and securing Plaintiffs' and Class Members' PI, Defendants allowed thieves—to access and collect individuals' PI. Defendants failed to employ reasonable and appropriate measures to protect against unauthorized disclosure and access to Plaintiffs' and Class Members' PI. Defendants' data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

70. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data. The body of law created by the FTC recognizes that failure to restrict access to information[52] and failure to segregate access to information[53] may violate the FTC Act.

71. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data, including driver's license numbers and other motor vehicle records (i.e., PI) constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

---

[51] *See Privacy and Security Enforcement Press Releases*, Federal Trade Commission, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last accessed Sept. 14, 2022).

[52] *In the Matter of LabMD, Inc.*, Dkt. No. 9357, Slip Opinion, at 15 ("Procedures should be in place that restrict users' access to only that information for which they have a legitimate need."), https://www.ftc.gov/system/files/documents/cases/160729labmd-opinion.pdf (last accessed Sept. 14, 2022).

[53] *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 258 (3d Cir. 2015) (companies should use "readily available security measures to limit access between" data storage systems).

E. Defendants Contravene the Purpose of the Driver's Privacy Protection Act

72. Prior to the enactment of the Driver's Privacy Protection Act, Congress found that most states freely turned over DMV information to whomever requested it with only few restrictions. 137 Cong. Rec. 27,327 (1993).

73. Due to these state lack of restrictions, Congress grew concerned that potential criminals could easily access home addresses and telephone numbers of potential victims. 140 Cong. Rec. 7929 (1994) (statement of Rep. Porter Goss).

74. These concerns did, in fact, materialize in the occurrence of crime, harassment, and stalking. Most notably, in 1989, a stalker shot and killed Rebecca Schaeffer, an upcoming actress, after obtaining her unlisted home address from the California DMV. 137 Cong. Rec. 27,327 (1993). In advocating for the DPPA, Representative Jim Moran (D-VA) recounted thieves using information from the DMV to learn home addresses and commit burglary and theft. 137 Cong. Rec. 27,327 (1993). Similarly, Senator Barbara Boxer (D-CA) explained how a man used the DMV to obtain the home addresses of several young women and sent them harassing letters. 39 Cong. Rec. 29,466 (1993). In another instance, a woman who visited a clinic that performed abortions found black balloons outside her home after a group of anti-abortion activists sought to harass her upon seeing her car in the clinic's parking lot. 139 Cong. Rec. 29,462 (1993) (statement of Sen. Chuck Robb).

75. In light of public outrage over the Schaeffer murder and growing concern over the threat to public safety posed by free access to DMV records, Congress enacted the DPPA "to protect the personal privacy and safety of licensed drivers consistent with the legitimate needs of business and government." S. Res. 1589, 103rd Cong. §1(b), 139 Cong. Rec. 26,266 (1993) (enacted).

76. Additionally, in enacting the DPPA, Congress was motivated by its "[c]oncern[] that personal information collected by States in the licensing of motor vehicle drivers was being released – even sold – with resulting loss of privacy for many persons." *Akkawi v. Sadr*, 2:20-CV-01034-MCE-AC, 2021 WL 3912151, at *4 (E.D. Cal. Sept. 1, 2021) (citing *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013) (alterations in original)). The sale of private information like driver's license numbers and other motor vehicle records was the exact impetus for the DPPA's passage.

77. As such, Congress sought to expressly prohibit "disclosing personal information obtained by the department in connection with a motor vehicle record." *Chamber of Commerce of United States v. City of Seattle*, 274 F. Supp. 3d 1140, 1154 (W.D. Wash. 2017). Driver's license numbers are thus explicitly listed as "personal information" from "motor vehicle records" under the DPPA. *See* 18 U.S.C. 2725(1).

78. The DPPA further states that "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title." 18 U.S.C. 2722(a). By making the PI of Plaintiffs and the Class publicly available to anyone who sought a quote, Defendants knowingly disclosed the PI of Plaintiff and Class Members and otherwise ran afoul of the purpose of the DPPA, and threatened the privacy and safety of licensed drivers, for whose protection the statute was enacted. Defendants' actions constituted a concrete injury and particularized harm to Plaintiffs and members of the Class, that would not have happened but for Defendants' failure to comply with the DPPA. Plaintiffs were harmed by the public disclosure of their private facts in addition to the other harms enumerated herein.

F. Plaintiffs' Injuries—Attempts to Secure PI After the Disclosure.

79. Defendants admitted there was unauthorized access to and disclosure of Plaintiffs' and Class Members' PI in the Notice Letter, as well as that Plaintiffs' and Class Members' PI was

likely viewed and copied off of Defendants' computer networks.[54] In the letter, Defendants also recognized that the unauthorized access and disclosure created substantial and present harm to Plaintiffs and Class Members—and specifically directed Plaintiffs and Class Members to mitigate their damages by "remain[ing] vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You should promptly report any activity indicative of identity theft or fraud immediately to law enforcement."[55]

80. Defendants also offered a year of credit monitoring due to the substantial and present risk to Plaintiffs and Class Members.[56] Plaintiffs and Class Members have been, and will continue to be, injured because they are now forced to spend time monitoring their credit and governmental communications—per Defendants' instructions, guarding against identity theft, and resolving fraudulent claims and charges because of Defendants' actions and/or inactions.

81. Here, Plaintiffs and Class Members suffered a loss of privacy; incurred costs and spent significant time, effort, and resources addressing the Unauthorized Data Disclosure; and are subject to an increased risk of identity theft and fraud as a result of the Unauthorized Data Disclosure. Similar injuries have been judicially recognized as actionable in federal court.[57]

---

[54] *Notice of Data Breach, supra* notes 5, 16, 17.
[55] *Id.*
[56] *Id.*
[57] See *In re: USAA Data Security Litigation*, Case No. 21-cv-5813 (VB), 2022 WL 3348527 (S.D.N.Y. Aug. 12, 2022), holding plaintiffs adequately pled and had standing on three separate grounds: (1) loss of privacy pursuant to their DPPA claim under the standards articulated in *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190, 2204 (2021); (2) they incurred costs and spent significant time, effort, and resources addressing the unauthorized data disclosure, which are sufficiently concrete injuries for purposes of Article III standing; and (3) they are subject to an increased risk of identity theft or fraud as a result of the unauthorized data disclosure sufficient to constitute an independent injury-in-fact.

Plaintiff Cardenas

82. Plaintiff Cardenas received the Notice Letter via email on or about June 7, 2022, from Defendants that they improperly exposed his PI to unauthorized third parties. Plaintiff Cardenas sought an insurance quote using Defendants' online platform but has never purchased insurance from Elephant.

83. Following the Unauthorized Data Disclosure in April 2022, Plaintiff Cardenas received notice that his driver's license number was for sale on the dark web. He received this notice because Plaintiff Cardenas was part of the Equifax breach, and signed up for credit monitoring as part of the settlement reached in that case. Plaintiff Cardenas had previously frozen his credit as a result of the Equifax breach and had received no notice of identity fraud or theft until the notice related to his driver's license number after the Unauthorized Data Disclosure.

84. Upon receiving notice of the above, and the Notice Letter from Defendants, Plaintiff Cardenas spent time researching his options to respond to the theft of his driver's license, and the use of same to commit identity fraud by putting his license number on the dark web. He spent and continues to spend additional time reviewing his credit and financial documents concerning the security of his identity. This is time Plaintiff Cardenas otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

85. Additionally, Plaintiff Cardenas has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. He deletes any and all unencrypted, non-password protected electronic documents containing his PI and destroys any documents that contain any of his PI, or that may contain any information that could otherwise be used to compromise his PI.

86. Plaintiff Cardenas suffered actual injury from having his PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) identity fraud; (b) loss of his

privacy; and (c) imminent and impending further injury arising from the increased risk of fraud and identity theft.

87. The identity theft suffered by Plaintiff Cardenas is logically and temporally linked to the Unauthorized Data Disclosure in the same way that other data breach cases have found to be "fairly traceable." His driver's license number was stolen shortly before he received a notice that his information was available for sale on the dark web, proof that his identity has been stolen.

88. As a result of the Unauthorized Data Disclosure, Plaintiff Cardenas was a victim of identity theft, and will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Bias

89. Plaintiff Bias received the Notice Letter around May 26, 2022, via the mail. The Notice Letter, which was dated May 23, 2022, said that Defendants improperly exposed her PI to unauthorized third parties. Plaintiff Bias may have sought an insurance quote using Defendants' online platform but has never purchased insurance from Elephant.

90. Upon receiving notice of the Notice Letter from Defendants, Plaintiff Bias spent time researching her options to respond to the theft of her driver's license. She spent and continues to spend additional time reviewing her credit and financial documents concerning the security of her identity. This is time Plaintiff Bias otherwise would have spent performing other activities, such as her job and/or leisurely activities for the enjoyment of life.

91. Additionally, Plaintiff Bias has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. She deletes any and all unencrypted, non-password protected electronic documents containing her PI and destroys any documents that contain any of her PI, or that may contain any information that could otherwise be used to compromise her PI.

Plaintiff Bias has never received a notice that her driver's license number or other PI was compromised in any other data breach or unauthorized data disclosure.

92. Plaintiff Bias suffered actual injury from having her PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) identity theft; (b) loss of her privacy; and (c) imminent and impending further injury arising from the increased risk of fraud and identity theft.

93. As a result of the Unauthorized Data Disclosure, Plaintiff Bias will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Holmes

94. Plaintiff Holmes received the Notice Letter dated June 3, 2022, from Defendants that they improperly exposed his PI to unauthorized third parties.

95. Prior to receiving the Notice Letter from Defendants, Plaintiff Holmes had never heard of the Defendants, nor had he had any contact with the Defendants. In fact, Plaintiff Holmes only visited Defendants' website after receiving the Notice Letter to determine who Defendants were and why they were contacting him.

96. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Holmes faces, Defendants offered him a 12-month subscription to a credit monitoring service. However, Plaintiff Holmes did not sign up for the program, because he does not trust that chosen vendor can protect his information. Moreover, traditional credit monitoring will not protect against the likely identity theft harm that will result from a compromised driver's license.

97. In mid-June 2022, Plaintiff Holmes began experiencing an uptick in spam text and telephone calls that he attributes to this Data Breach. Spam texts include unauthorized third-parties

attempting to see Plaintiff Holmes insurance policies. Spam telephone calls include unauthorized third-parties posing as debt collectors attempting to collect fictional debts from Plaintiff Holmes.

98. On or about June 21, 2022—after the Unauthorized Data Disclosure in April 2022—Plaintiff Holmes received notice from his identity theft protection service that his driver's license number was "found" on the dark web.

99. Upon receiving notice of the above, and the Notice Letter from Defendants, Plaintiff Holmes spent time researching his options to respond to the theft of his driver's license, and the use of same to commit identity fraud by putting his license number on the dark web. As of the time he filed his complaint, he had spent approximately eight hours reviewing his bank, credit, and debit card statements. Moreover, Plaintiff Holmes spent this time at Defendants' direction. Indeed, in the notice letter Plaintiff Holmes received, Defendants directed him to spend time mitigating his losses by "reviewing your account statements and free credit reports for suspicious activity[.]" Plaintiff Holmes also plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Unauthorized Data Disclosure, including continually reviewing his depository, credit, and other accounts for any unauthorized activity. This amount of time will increase, and is time Plaintiff Holmes otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

100. Additionally, Plaintiff Holmes has never knowingly transmitted unencrypted PI over the internet or any other unsecured source, and stores any documents containing his PI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for her various online accounts.

101. Plaintiff Holmes suffered actual injury from having his PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) identity fraud; (b) loss of his

privacy; (c) imminent and impending further injury arising from the increased risk of fraud and identity theft; and (d) significant fear, anxiety, and stress, which has been compounded by the fact that Defendants have not been forthright with information about the Unauthorized Data Disclosure.

102. The identity theft suffered by Plaintiff Holmes is logically and temporally linked to the Unauthorized Data Disclosure in the same way that other data breach cases have found to be "fairly traceable." His driver's license number was stolen shortly before he received a notice that his information was on the dark web, proof that his identity has been stolen.

103. As a result of the Unauthorized Data Disclosure, Plaintiff Holmes was a victim of identity theft, and will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Robert Shaw

104. Plaintiff Shaw received coverage under an insurance policy issued by Defendants from on or about December 16, 2018 until on or about December 16, 2019.

105. As a condition of receiving insurance, Defendants required Plaintiff Shaw to disclose personal information ("PI"), sometimes referred to as personally identifiable information ("PII"), which included, but was not limited to, Social Security Number, driver's license number, name, address, telephone number, and or medical or disability information. Defendants acknowledge this in their privacy policy when they characterize the information they collect, PI and or PHI, including driver's license numbers and dates of birth, as "Nonpublic Personal Information."

106. Plaintiff Shaw chose not to renew his policy with Defendants after on or about December 16, 2019.

107. Plaintiff Shaw received a Notice Letter dated May 23, 2022 from Defendants concerning the Data Breach. The compromised files, which Defendants obtained from motor vehicle records, included Plaintiff Shaw's full name and driver's license number, and may have also included his date of birth, address, and any other sensitive PII Defendants obtained at the time of the breach.

108. The Notice Letter also states, "In April, 2022, we identified unusual activity on our network," yet the letter does not specify when in April such activity was identified.

109. The Notice Letter further states a "comprehensive investigation" was conducted and "on April 25, 2022, our review determined your information was in that affected data."

110. Plaintiff Shaw greatly values his privacy and PII. Prior to the Data Breach, Plaintiff Shaw took reasonable steps to maintain the confidentiality of his PII.

111. Plaintiff Shaw received a letter dated May 23, 2022 from Defendants concerning the Data Breach. The letter states that unauthorized actors gained access to files on Defendants' network from March 26, 2022 through April 1, 2022. The compromised files contained full names and driver's license numbers.

112. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Shaw faces, Defendants offered him a 12 month subscription to a credit monitoring service. Plaintiff Shaw has not signed up for the program, however, because he does not trust the chosen vendor can protect his information. Moreover, traditional credit monitoring will not protect against the likely identity theft harm that will result from a compromised driver's license.

113. Since learning of the Data Breach, Plaintiff Shaw has spent additional time reviewing his bank statements, tax information, car titles, and credit card statements. Moreover, Shaw spent this time at Defendants' direction. Indeed, in the notice letter Plaintiff Shaw received,

Defendant directed him to spend time mitigating his losses by "reviewing your account statements and free credit reports for suspicious activity[.]"

114. The Data Breach has caused Plaintiff Shaw to suffer significant fear, anxiety, and stress, which has been compounded by the fact that Defendants have not been forthright with information about the Data Breach.

115. Plaintiff Shaw plans on taking additional time-consuming, necessary steps to help mitigate the harm caused by the Data Breach, including continually reviewing his depository, credit, tax information, car titles, and other accounts for any unauthorized activity.

116. Additionally, Plaintiff Shaw is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

117. Plaintiff Shaw stores any documents containing his PII in a secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

118. Plaintiff Shaw has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendants' possession, is protected and safeguarded from future breaches.

G. Plaintiffs and Class Members Suffered Additional Damages.

119. Plaintiffs and Class Members are at ongoing risk for actual identity theft in addition to all other forms of fraud.

120. The ramifications of Defendants' disclosure and failure to keep individuals' PI secure are long lasting and severe. Once PI is disseminated to unauthorized parties, fraudulent use of that information and damage to victims may continue for years.[58]

121. Plaintiffs' and Class Members' PI is private, valuable, and sensitive in nature as it can be used to commit a lot of different harms and fraud in the hands of the wrong people. Defendants failed to obtain Plaintiffs' and Class Members' consent to disclose such PI to any other person, as required by applicable law and industry standards.

122. Defendants' inattention to the reality that anyone, especially thieves with various pieces of individuals' PI, could obtain any individual's PI through compromise of Defendants' computer systems left Plaintiffs and Class Members with no ability to protect their sensitive and private information.

123. Defendants had the resources necessary to prevent the Unauthorized Data Disclosure, but neglected to adequately implement data security measures, despite their obligations to protect Plaintiffs' and Class Members' PI from unauthorized disclosure.

124. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, it would have prevented the unauthorized access, disclosure, and ultimately, the theft of PI.

125. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would

[58] *2014 LexisNexis True Cost of Fraud Study*, LexisNexis (August 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Sept. 14, 2022).

have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Unauthorized Data Disclosure on their lives.

126. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[59]

127. As a result of Defendants' failure to prevent the Unauthorized Data Disclosure, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. the compromise, publication, theft, and/or unauthorized use of their PI;

b. out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. compromise of their credit scores, access to credit, and other financial scores as a result of identity theft and compromised financial and driver's license information;

[59] Erika Harrell, Ph.D. and Lynn Langton, Ph.D., *Victims of Identity Theft, 2012*, U.S. Department of Justice (December 2013), https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed Sept. 14, 2022).

e. inability to access government services such as tax refunds or unemployment benefits because compromise of those accounts not only causes fraud but also makes it impossible to make legitimate claims;

f. the continued risk to their PI, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PI in their possession; and

g. current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Unauthorized Data Disclosure for the remainder of the lives of Plaintiffs and Class Members.

128. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring that their PI is secure, remains secure, and is not subject to further misappropriation and theft.

129. To date, other than providing 12 months of credit monitoring and identity protection services, none of which is targeted to driver's license information or designed to combat unemployment benefits fraud, Defendants do not appear to be taking any measures to assist Plaintiffs and Class Members other than simply telling them to do be vigilant themselves.

130. Defendants' failure to adequately protect Plaintiffs' and Class Members' PI has resulted in Plaintiffs and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Instead, as Defendants' Notice indicates, they are putting the burden on Plaintiffs and Class Members to discover possible fraudulent activity and identity theft.

131. Defendants' offer of 12 months of identity monitoring and identity protection services to Plaintiffs and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when additional harm occurs versus when it is discovered, and also between when PI is acquired and when it is used.

CLASS ACTION ALLEGATIONS

132. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and the following proposed Nationwide Class as defined as follows:

> All persons in the United States whose PI was compromised in the Unauthorized Data Disclosure announced by Defendants on or near May 6, 2022 (the "Nationwide Class").

133. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiffs Cardenas and Holmes seek certification of the following Texas state subclass:

> All persons in Texas whose PI was compromised in the Unauthorized Data Disclosure announced by Defendants on or near May 6, 2022 ("Texas Subclass").

134. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiff Bias seeks certification of the following Illinois state subclass:

> Illinois Subclass: All persons in Illinois whose PI was compromised in the Unauthorized Data Disclosure announced by Defendants on or near May 6, 2022 ("Illinois Subclass").

135. The Nationwide Class, and Texas and Illinois Subclasses are collectively referred to herein as "Class" unless otherwise stated.

136. Excluded from the proposed Class are any officer or director of Defendants; any officer or director of any affiliate, parent, or subsidiary of Defendants; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

137. **Numerosity.** Members of the proposed Class likely number in the millions and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendants' own records.

138. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants' inadequate data security measures were a cause of the Unauthorized Data Disclosure;

c. Whether Defendants' actions were knowing in improperly disclosing driver's license numbers to unauthorized parties and/or entities;

d. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiffs and the other Class Members to exercise due care in collecting, storing, and safeguarding their PI;

e. Whether Defendants disclosed PI obtained from the records of Defendants or third parties without the permission or consent of Plaintiffs and the Class;

f. Whether Plaintiffs and the Class are at an increased risk for identity theft because of the data security breach;

g. Whether Defendants violated the Drivers' Privacy Protection Act, 18 U.S.C. § 2724,

h. Whether Defendants were negligent;

i. Whether Plaintiffs and the Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief; and

j. Whether Plaintiffs and the Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

139. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved predominate over any individualized issues. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

140. **Typicality:** Plaintiffs' claims are typical of the claims of the members of the Class. All Class Members were subject to the Unauthorized Data Disclosure and had their PI accessed by, used and/or disclosed to unauthorized third parties. Defendants' misconduct impacted all Class Members in the same manner.

141. **Adequacy of Representation:** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members they seek to represent; they retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

142. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the Class Members pale compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not.

Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

143. **Injunctive and Declaratory Relief:** Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2) because Defendants, through their uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, Defendants continue to maintain their inadequate security practices, retain possession of Plaintiffs' and Class Members' PI, and have not been forced to change their practices or relinquish PI by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

144. Likewise, particular issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. whether Plaintiffs' and Class Members' PI was accessed and/or acquired by an unauthorized party because of the data security breach;

b. whether Defendants owed a legal duty to Plaintiffs and Class Members;

c. whether Defendants' actions were knowing in improperly disclosing driver's license numbers to unauthorized parties and/or entities;

d. whether Defendants failed to take adequate and reasonable steps to safeguard Plaintiffs' and Class Members' PI;

e. whether Defendants failed to adequately monitor their data security systems;

f. whether Defendants failed to comply with applicable laws, regulations, and/or industry standards relating to data security amounting to negligence;

g. whether Defendants' security measures were reasonable in light of data security recommendations, and other measures recommended by data security experts;

h. whether Defendants knew or should have known they did not employ adequate and reasonable measures to keep Plaintiffs' and Class Members' PI secure; and

i. whether Defendants' failure to adhere to FTC data security obligations, industry standards, and/or measures recommended by data security experts caused the Data Breach.

CAUSES OF ACTION

First Cause of Action

Violation of the Drivers' Privacy Protection Act ("DPPA"), 18 U.S.C. § 2721, *et seq.* (On behalf of Plaintiffs, the Nationwide Class, and the Texas and Illinois Subclasses)

145. Plaintiffs incorporate the above allegations by reference.

146. The DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains." 18 U.S.C. § 2724.

147. Under the DPPA, "person" is defined as "an individual, organization, or entity." 18 U.S.C. 2725(2). Defendant is a "person" under the DPPA.

148. Further, the definition of "disclose" is "to make known or public" or "expose to view." [60] Defendants' voluntary action of exposing Plaintiffs' and Class Members' PI constitutes a knowing disclosure. In particular, Defendants intentionally configured and designed their online

[60] https://www.merriam-webster.com/dictionary/disclose (Last accessed Sept. 14, 2022).

insurance quoting platform to generate responses to requests for insurance quotes that included PI from motor vehicle records. In doing so, unauthorized actors were able to access and obtain the PI of Plaintiffs and Class Members for nefarious purposes.

149. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

150. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.'" 18 U.S.C. § 2725(1). Drivers' license numbers are motor vehicle records and personal information under the DPPA. 18 U.S.C. § 2725(3); *see also Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 943 (7th Cir. 2015).

151. Defendants obtain, use, disclose, resell, and redisclose motor vehicle records from their customers.

152. Defendants also obtain motor vehicle records directly from state agencies or through resellers who sell such records.

153. Defendants knowingly used motor vehicle records for uses not permitted by the statute, including sales, and marketing, among other impermissible uses.

154. Defendants knowingly and voluntarily configured and designed their computer systems and/or linked their respective public websites to systems and/or networks storing, maintaining, and/or obtaining Plaintiffs' and Class Members' PI, including the application website, which resulted in the disclosure of Plaintiffs' and Class Members' PI to anyone who requested an insurance quote, in direct violation of the DPPA.

155. Defendants failed to use reasonable care in protecting Plaintiffs' and Class Members' PI by installing substandard security measures that failed to protect it, and voluntarily disclosed it to cyber criminals through the intentional configuration and design of its online insurance quoting platform.

156. Further, Defendants had actual and/or constructive notice of the risk to Plaintiffs' and the Class Members' PI because they should have been aware that failing to incorporate basic security measures in the configuration and design of their online insurance quoting platform, such as authentication of the person requesting the quote, would cause the improper disclosure of Plaintiffs' and Class Members' PI.

157. During the period starting March 26, 2022, PI, including drivers' license numbers and other information from motor vehicle recoreds, of Plaintiffs and Class Members, are available to thieves and have been removed from Defendants' computer systems. Defendants knowingly used and disclosed and/or redisclosed Plaintiffs' and Class Members' motor vehicle records and PI to thieves, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

158. As a result of the Unauthorized Data Disclosure, Plaintiffs and putative Class Members are entitled to actual damages, liquidated damages, punitive damages, attorneys' fees and costs.

Second Cause of Action

Negligence
(On behalf of Plaintiffs, the Nationwide Class, and the Texas and Illinois Subclasses)

159. Plaintiffs incorporate the above allegations by reference.

160. Defendants owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members'

PI from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, implementing, maintaining, and testing their data security systems to ensure Plaintiffs' and Class Members' PI in Defendants' possession, or that could be accessed by Defendants, was adequately secured and protected.

161. Defendants owed a duty of care to Plaintiffs and Members of the Class to provide security, consistent with industry standards, to ensure that their systems and networks adequately protected PI they stored, maintained, used, and/or obtained.

162. Defendants owed a duty of care to Plaintiffs and Members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in having inadequate data security for private PI without the consent or authorization of the person whose PI was being provided.

163. Unbeknownst to Plaintiffs and Class Members, they were entrusting Defendants with their PI when Defendants obtained their PI from motor vehicle records directly from state agencies or through resellers who sell such records, as well as through other channels. Defendants had an obligation to safeguard Plaintiffs' and Class Members' information and were in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Unauthorized Data Disclosure.

164. In addition, Defendants required Plaintiffs and Class Members to submit sensitive personal information, including their PI, in order to obtain insurance. Defendants stored this vast treasure trove of PI on unsecured and inadequate computer networks.

165. By collecting, storing, using, and profiting from this data, Defendants each had a duty of care to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting this PI in Defendants' possession from being

compromised, lost, stolen, accessed, and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Defendants' security systems and data storage architecture to ensure that Plaintiffs' and Class Members' PI was adequately secured and protected; (b) implementing processes that would detect an unauthorized breach of Defendants' security systems and data storage architecture in a timely manner; (c) timely acting upon all warnings and alerts, including public information, regarding Defendants' security vulnerabilities and potential compromise of the compiled data of Plaintiffs and millions of Class Members; and (d) maintaining data security measures consistent with industry standards.

166. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their PI. Defendants' misconduct included failing to implement the systems, policies, and procedures necessary to prevent the Unauthorized Data Disclosure.

167. Defendants acknowledge their conduct created actual harm to Plaintiffs and Class Members because Defendants warned of the potential for identity theft as a result of the Unauthorized Data Disclosure, and offered one year of credit monitoring.

168. Defendants knew, or should have known, of the risks inherent in collecting and storing PI and the importance of adequate security. Defendants knew about—or should have been aware of—numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

169. Defendants breached their duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard Plaintiffs' and Class Members' PI.

170. Because Defendants knew that a breach of their systems would damage millions of individuals whose PI was inexplicably stored or was accessible, including Plaintiffs and Class

Members, Defendants had a duty to adequately protect their data systems and the PI contained and/or accessible therein.

171. Defendants also had independent duties under state and federal laws requiring Defendants to reasonably safeguard Plaintiffs' and Class Members' PI.

172. Defendants also had common law duties to prevent foreseeable harm to Plaintiffs and Class Members. These duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their PI because hackers routinely attempt to steal such information and use it for nefarious purposes, Defendants knew that it was more likely than not Plaintiffs and other Class Members would be harmed by such theft.

173. Defendants had a duty to monitor, supervise, control, or otherwise provide oversight to safeguard the PI that was collected and stored Defendants' computer networks.

174. Defendants' duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiffs and Class Members, on the other hand. The special relationship arose because Plaintiffs and Class Members entrusted Defendants with their PI as part of the applications for, opening, or use of insurance services with Defendants. Defendants alone could have ensured that their security systems and data storage architecture were sufficient to prevent or minimize the Unauthorized Data Disclosure.

175. Defendants' duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PI. Various FTC publications

and data security breach orders further form the basis of Defendants' duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

176. Defendants knew or should have known that their computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential PI.

177. Defendants breached the duties they owed to Plaintiffs and Class Members described above and thus were negligent. Defendants breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PI of Plaintiffs and Class Members; (b) detect the breach while it was ongoing or promptly after it occurred; (c) maintain security systems consistent with industry standards; and (d) promptly notify Plaintiffs and Class Members.

178. In engaging in the negligent acts and omissions as alleged herein, which permitted thieves to access Defendants' systems that stored and/or had access to Plaintiffs' and Class Members' PI, Defendants violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce." This includes failing to have adequate data security measures and failing to protect Plaintiffs' and the Class Members' PI.

179. Plaintiffs and the Class Members are among the class of persons Section 5 of the FTC Act was designed to protect, and the injuries suffered by Plaintiffs and Class Members are the types of injury Section 5 of the FTC Act was intended to prevent.

180. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and Class Members, their PI would not have been compromised.

181. Neither Plaintiffs nor the other Class Members contributed to the Unauthorized Data Disclosure as described in this Complaint.

182. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or theft of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports, compromises to credit scores, and access to state and tax benefits and refunds; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PI, which remains in Defendants' possession (and/or Defendants had access to) and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PI in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PI.

Third Cause of Action

Negligence *Per Se*
(On behalf of Plaintiffs, the Nationwide Class, and the Texas and Illinois Subclasses)

183. Plaintiffs incorporate the above allegations by reference.

184. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect PI. Various FTC publications and orders also form the basis of Defendants' duty.

185. Defendants violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PI and not complying with industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PI obtained and stored and the foreseeable consequences of a data breach on Defendants' systems.

186. Defendants' duty to use reasonable security measures also arose under the DPPA, under which Elephant was required to protect the privacy, confidentiality, and integrity of driver's license information and only to use driver's license information in a permissible fashion.

187. Defendants' violation of Section 5 of the FTC Act (and similar state statutes) along with the DPPA constitutes negligence *per se*.

188. Plaintiffs and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes), and the DPPA, were intended to protect.

189. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) and the DPPA were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members. The DPPA was similarly enacted as a direct result of failures to protect consumer privacy like those outlined above.

190. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PI; illegal sale of the

compromised PI on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Unauthorized Data Disclosure reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PI; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

Fourth Cause of Action

Unjust Enrichment
(On behalf of Plaintiffs, the Nationwide Class, and the Texas and Illinois Subclasses)

191. Plaintiffs incorporate the above allegations by reference.

192. Plaintiffs and Class Members have an interest, both equitable and legal, in the PI about them that was conferred upon, collected by, and maintained by Defendants and that was ultimately stolen in the Unauthorized Data Disclosure.

193. Defendants were benefitted by the conferral upon them of the PI pertaining to Plaintiffs and Class Members and by their ability to retain, use, and profit from that information. Defendants understood that they were in fact so benefitted and state so on their website when they state they use PI to market additional products to both Plaintiffs and Class Members and to the general public.[61]

194. Defendants also understood and appreciated that the PI pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon Defendants maintaining the privacy and confidentiality of that PI.

[61] *See Elephant Insurance Privacy Notice, supra* note 2.

195. But for Defendants' willingness and commitment to maintain Plaintiffs' privacy and confidentiality, Plaintiffs would not have transferred their PI to and entrusted it with Defendants.

196. Defendants continue to benefit and profit from their retention and use of the PI while its value to Plaintiffs and Class Members has been diminished.

197. Defendants also benefitted through its unjust conduct by retaining money gained through their practice of collecting PI from the Plaintiffs and Class Members and providing inadequate data privacy and security that they should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PI.

198. It is inequitable for Defendants to retain these benefits.

199. As a result of Defendants' wrongful conduct as alleged in this Complaint (including, among things, their knowing failure to employ adequate data security measures, their continued maintenance and use of the PI belonging to Plaintiffs and Class Members without having adequate data security measures, and their other conduct facilitating the theft of that PI), Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members.

200. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Members' PI, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

201. Under the common law doctrine of unjust enrichment, it is inequitable for Defendants to be permitted to retain the benefits they received, and are still receiving, without justification, from Plaintiffs and Class Members (in the form of PI belonging to Plaintiffs and the

Class Members that is being used for marketing and profitable purposes by Defendants) in an unfair and unconscionable manner. Defendants' retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

202. The benefits conferred upon, received, and enjoyed by Defendants were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendants to retain these benefits.

203. Plaintiffs have no adequate remedy at law.

204. Defendants are therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on Defendants as a result of their wrongful conduct, including specifically: the value to Defendants of the PI that was stolen in the Unauthorized Data Disclosure; the profits Defendants are receiving from the use of that information; the amounts that Defendants overcharged Plaintiffs and/or Class Members for use of their insurance services; and the amounts that Defendants should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PI.

Fifth Cause of Action

Violation of the Texas Consumer Protection Act,
Texas Bus. & Com. Code §§ 17.41, et seq.
(On behalf of Plaintiffs Cardenas and Holmes and the Texas Subclass)

205. Plaintiffs incorporate the above allegations by reference.

206. Defendants are "person[s]" as defined by Tex. Bus. & Com. Code § 17.45(3).

207. Plaintiffs Cardenas and Holmes and the Texas Subclass members are "consumer[s]" as defined by Tex. Bus. & Com. Code § 17.45(4).

208. Defendants advertised, offered, or sold services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

209. Defendants engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including: representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities they do not have; representing that goods or services are of a particular standard, quality or grade, if they are of another; and/or advertising goods or services with intent not to sell them as advertised.

210. The Defendants' false, misleading, and deceptive acts and practices include:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Texas Subclass members' PI, which was a direct and proximate cause of the Unauthorized Data Disclosure;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Unauthorized Data Disclosure;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Cardenas' and Holmes' and Texas Subclass members' PI, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Unauthorized Data Disclosure;

d. misrepresenting that they would protect the privacy and confidentiality of Plaintiffs Cardenas' and Holmes' and Texas Subclass members' PI, including by implementing and maintaining reasonable security measures;

e. misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Cardenas' and Holmes' and

Texas Subclass members' PI, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs Cardenas' and Holmes' and Texas Subclass members' PI; and

g. omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs Cardenas' and Holmes' and Texas Subclass members' PI, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the DPPA, 18 U.S.C. § 2724.

211. Defendants intended to mislead Plaintiffs Cardenas and Holmes and Texas Subclass members and induce them to rely on their misrepresentations and omissions.

212. The Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of the Defendants' data security and ability to protect the confidentiality of consumers' PI.

213. Had Defendants disclosed to Plaintiffs Cardenas and Holmes and Class Members that their data systems were not secure and, thus, vulnerable to attack, and that Defendants failed to protect sensitive driver's license information, Defendants would have been unable to continue in business and would have been forced to adopt reasonable data security measures and comply with the law. Instead, the Defendants received, maintained, and compiled Plaintiffs Cardenas' and Holmes' and Class Members' PI as part of the services the Defendants provided without advising Plaintiffs Cardenas and Holmes and Class Members that the Defendants' data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs Cardenas' and Holmes'

and Class Members' PI. Accordingly, Plaintiffs Cardenas and Holmes and the Texas Subclass members acted reasonably in relying on the Defendants' misrepresentations and omissions, the truth of which they could not have discovered.

214. The Defendants had a duty to disclose the above facts due to the circumstances of this case and the sensitivity and extensivity of the PI in their possession. This duty arose because Plaintiffs Cardenas and Holmes and the Texas Subclass members reposed a trust and confidence in the Defendants when they provided their PI to the Defendants in exchange for the Defendants' services. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs Cardenas and Holmes and the Texas Subclass, and the Defendants because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in the Defendants. The Defendants' duty to disclose also arose from their: possession of exclusive knowledge regarding the security of the PI; active concealment of the state of their security; and/or incomplete representations about the security and integrity of their computer and data storage systems, while purposefully withholding material facts from Plaintiffs Cardenas and Holmes and the Texas Subclass that contradicted these representations and omissions.

215. Defendants engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Defendants engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

216. Consumers, including Plaintiffs Cardenas and Holmes and Texas Subclass members, lacked knowledge about deficiencies in Defendants' data security because this information was known exclusively by Defendants. Consumers also lacked the ability, experience,

or capacity to secure the PI in Defendants' possession or to fully protect their interests with regard to their data. Plaintiffs Cardenas and Holmes and Texas Subclass members lack expertise in information security matters and do not have access to Defendants' systems in order to evaluate their security controls. Defendants took advantage of their special skill and access to the PI to hide their inability to protect the security and confidentiality of Plaintiffs Cardenas and Holmes and Texas Subclass members' PI.

217. Defendants intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Defendants' conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Unauthorized Data Disclosure, which resulted from Defendants' unconscionable business acts and practices, exposed Plaintiffs Cardenas and Holmes and Texas Subclass members to a wholly unwarranted risk to the safety of their PI and the security of their identity or credit, and worked a substantial hardship on consumers. Plaintiffs Cardenas and Holmes and Texas Subclass members cannot mitigate this unfairness because they cannot undo the Unauthorized Data Disclosure.

218. As a direct and proximate result of Defendants' unconscionable and deceptive acts or practices, Plaintiffs Cardenas and Holmes and the Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with and overcharges by Defendants, as they would not have paid Defendants for services or would have paid less for such services but for the violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial

accounts for fraudulent activity; loss of value of their PI; and an increased, imminent risk of fraud and identity theft.

219. Defendants' unconscionable and deceptive acts or practices were a producing cause of Plaintiffs Cardenas' and Holmes' and Texas Subclass members' injuries, ascertainable losses and economic and non-economic damages.

220. Defendants' violations present a continuing risk to Plaintiffs Cardenas and Holmes and Texas Subclass members as well as to the general public.

221. Plaintiffs Cardenas and Holmes and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; treble damages for each act committed intentionally or knowingly; restitution; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

Sixth Cause of Action

Violation of the Illinois Consumer Fraud Act, 815 ILCS §§ 505, *et seq*.
(On behalf of Plaintiffs and the Illinois Subclass)

222. Plaintiffs incorporate the above allegations by reference.

223. This claim is brought under the laws of Illinois and on behalf of all other natural persons whose PI was compromised as a result of the Unauthorized Data Disclosure and reside in states having similar laws regarding consumer fraud.

224. Defendants are "persons" as defined by 815 Ill. Comp. Stat. §§ 505/1(c).

225. Plaintiff Bias and the Illinois Subclass Members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

226. Defendants' conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. § 505/1(f).

227. Defendants' deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and the Illinois Subclass Members' PI, which was a direct and proximate cause of the Unauthorized Data Disclosure;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Unauthorized Data Disclosure;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Illinois Subclass Members' PI, including duties imposed by the FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Unauthorized Data Disclosure;

d. misrepresenting that it would protect the privacy and confidentiality of Plaintiffs and the Illinois Subclass Members' PI, including by implementing and maintaining reasonable security measures;

e. misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and the Illinois Subclass Members' PI, including duties imposed by the FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp.

Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. failing to timely and adequately notify the Illinois Subclass Members of the Unauthorized Data Disclosure;

g. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the Illinois Subclass Members' PI;

h. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the Illinois Subclass Members' PI, including duties imposed by FCRA, FTC Act, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

i. failing to provide disclose the Unauthorized Data Disclosure in a timely fashion, in violation of 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

228. Defendants' representations and omissions were material because they were likely to deceive reasonable clients, applicants, and consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PI.

229. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and Illinois Subclass Members, into believing that their PI would not be exposed to unauthorized parties.

230. Defendants intended to mislead Plaintiffs and Illinois Subclass Members and induce them to rely on their misrepresentations and omissions.

231. The above unfair and deceptive practices and acts by Defendants offend public policy. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

232. Defendants acted intentionally and knowingly to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiffs' and Illinois Subclass Members' rights.

233. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive acts and practices, Plaintiffs and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including, but not limited to: actual identity theft and current and ongoing risk of identity fraud; loss of the opportunity to control how their PI is used; the compromise, publication, and/or theft of their PI; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PI; lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to:

a. efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

b. the current and ongoing risk to Plaintiffs' and Illinois Subclass Members' PI, which remains in Defendants' possession and subject to further unauthorized

disclosures, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Illinois Subclass Members' PI in Defendants' continued possession;

c. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PI accessed and acquired as a result of the Unauthorized Data Disclosure—which may take months if not years to discover, detect, and remedy;

d. future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their PI;

e. the diminished value of their PI;

f. other economic harm;

g. emotional distress; and

h. the necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

234. Plaintiffs and Illinois Subclass Members seek all monetary and non–monetary relief allowed by law, including damages, restitution, nominal and punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

Seventh Cause of Action

Violation of the Illinois Uniform Deceptive Trade Practices Act,
815 ILCS §§ 510/2, *et seq*.
(On behalf of Plaintiff Bias and the Illinois Subclass)

235. Plaintiffs incorporate the above allegations by reference.

236. This claim is brought under the laws of Illinois and on behalf of all Plaintiff Bias other natural persons whose PI was compromised as a result of the Unauthorized Data Disclosure and reside in states having similar laws regarding deceptive trade practices like Illinois.

237. Defendants are "persons" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

238. Defendants engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §§ 510/2(a), including: representing that goods or services have characteristics that they do not have; representing that goods or services are of a particular standard, quality, or grade if they are of another; advertising goods or services with intent not to sell them as advertised; and engaging in other conduct that creates a likelihood of confusion or misunderstanding.

239. Defendant's deceptive trade practices include:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Illinois Subclass members' PI, which was a direct and proximate cause of the Unauthorized Data Disclosure;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Unauthorized Data Disclosure;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bias's and Illinois Subclass members' PI, including duties imposed by the FTC Act, 15 U.S.C. § 45, as well as Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Unauthorized Data Disclosure;

d. misrepresenting that they would protect the privacy and confidentiality of Plaintiff Bias's and Illinois Subclass members' PI, including by implementing and maintaining reasonable security measures;

e. misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bias's and Illinois Subclass members' PI, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, the Personal Information Protection Act, 815 Ill. Comp. Stat § 530, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Bias's and Illinois Subclass members' PI;

g. failing to timely and adequately notify Plaintiff Bias and Illinois Subclass Members of the Unauthorized Data Disclosure; and

h. omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Bias's and Illinois Subclass members' PI, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the DPPA, 18 U.S.C. § 2724.

240. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of Plaintiff Bias's and Illinois Subclass Members' PI.

241. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff Bias and Illinois Subclass Members, into believing that their PI would not be exposed to unauthorized parties.

242. The above unfair and deceptive practices and acts by Defendants offend and violate public policy. These acts caused substantial injury to Plaintiff Bias and Illinois Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

243. As a direct and proximate result of Defendants' unfair, unlawful, and deceptive trade practices, Plaintiff Bias and Illinois Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including, but not limited to:

a. actual identity theft and current and ongoing risk of identity fraud;

b. loss of the opportunity to control how their PI is used;

c. the compromise, publication, and/or theft of their PI;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PI;

e. lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts,

closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports;

f. the current and ongoing risk to their PI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff Bias's and Illinois Subclass Members' PI in Defendants' continued possession;

g. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PI accessed and acquired as a result of the Unauthorized Data Disclosure—which may take months if not years to discover, detect, and remedy;

h. future out-of-pocket expenses associated with paying for fraudulent charges resulting from identity theft, and/or unauthorized use of their PI;

i. the diminished value of their PI;

j. other economic harm;

k. emotional distress;

l. and the necessity to engage legal counsel and incur attorneys' fees, costs, and expenses.

244. Plaintiff Bias and Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

Eighth Cause of Action

Declaratory and Injunctive Relief
(On behalf of Plaintiffs, the Nationwide Class, and the Texas and Illinois Subclasses)

245. Plaintiffs incorporate the above allegations by reference.

246. This Cause of Action is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

247. As previously alleged, Plaintiffs and Class Members had a reasonable expectation that companies, such as Defendants, who access their PI through automated systems and collect untold volumes of PI, would provide adequate security for that PI.

248. Defendants owed a duty of care to Plaintiffs and Class Members requiring it to adequately secure PI.

249. Defendants still possess PI regarding Plaintiffs and Class Members.

250. Since the Unauthorized Data Disclosure, Defendants announced few if any changes to their data security infrastructure, processes, or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Unauthorized Data Disclosure to occur and, thereby, prevent further attacks.

251. The Unauthorized Data Disclosure caused actual harm because of Defendants' failure to fulfill their duties of care to provide security measures to Plaintiffs and Class Members. Further, Plaintiffs and Class Members are at risk of additional or further harm due to the exposure of their PI and Defendants' failure to address the security failings that lead to such exposure.

252. There is no reason to believe that Defendants' security measures are more adequate now than they were before the Unauthorized Data Disclosure to meet Defendants' legal duties.

253. An actual controversy has arisen in the wake of the Unauthorized Data Disclosure regarding its present and prospective common law and other duties to reasonably safeguard its

customers' PI and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PI. Plaintiffs remain at ongoing and imminent risk that further compromises of their PI will occur in the future.

254. Plaintiffs, therefore, seek a declaration (1) that Defendants' existing security measures do not comply with their duties of care to provide adequate security, and (2) that to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. ordering Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors,

b. ordering Defendants engage third–party security auditors and internal personnel to run automated security monitoring,

c. ordering Elephant audit, test, and train its security personnel regarding any new or modified procedures,

d. ordering Defendants not to make PI available on any publicly-facing webpage, and to adequately secure PI in any website or network computer system,

e. ordering Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services,

f. ordering Defendants to conduct regular computer system scanning and security checks; and

g. ordering Defendants to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a disclosure when it occurs, and what to do in response to a breach.

255. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another unauthorized data disclosure by Defendants. The risk of another such disclosure is real, immediate, and substantial. If another disclosure occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

256. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another unauthorized data disclosure occurs because of Defendants, Plaintiffs and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have pre-existing legal obligations to employ such measures.

257. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data disclosure by Defendants, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose PI would be further compromised.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all others similarly situated, respectfully request the Court enter an order:

a. Certifying the proposed Class as requested herein,

b. Appointing Plaintiffs as Class Representatives and undersigned counsel as Class Counsel,

c. Finding that Defendants engaged in the unlawful conduct as alleged herein,

d. Granting injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

e. Awarding Plaintiffs and Class Members damages,

f. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest on all amounts awarded,

g. Awarding Plaintiffs and the Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

VI. DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the proposed Class of all others similarly situated, hereby demand a trial by jury as to all matters so triable pursuant to Rule 38 of the Federal Rules of Civil Procedure.

Dated: September 14, 2022

Respectfully submitted,

By: /s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP
300 N. Washington Street, Suite 404
Alexandria, VA 22314
Tel.: 888.987.9991
swebster@websterbook.com

Lee Floyd, VSB #88459
Justin M. Sheldon, VSB #82632
BREIT BINIAZAN, PC
2100 East Cary Street, Suite 310
Richmond, Virginia 23223
Tel.: 804.351.9040; Fax: 804.351.9170
Lee@bbtrial.com
Justin@bbtrial.com

Jeffrey A. Breit, VSB #18876
Kevin Biniazan, VSB #92019
BREIT BINIAZAN, P.C.
Towne Pavilion Center II
600 22nd Street, Suite 402
Virginia Beach, Virginia 23451
Tel.: 757.622.6000; Fax: 757.670.3939
Jeffrey@bbtrial.com
Kevin@bbtrial.com

Plaintiffs' Co-Lead Interim Liaison Class Counsel

Kate M. Baxter-Kauf (*Pro Hac Vice*)
Karen Hanson Riebel (*Pro Hac Vice*)
Maureen Kane Berg*
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Tel.: 612.339.6900; Fax: 612.339.0981
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com
mkberg@locklaw.com

M. Anderson Berry (*Pro Hac Vice*)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Tel.: 916.239.4778; Fax: 916.924.1829
aberry@justice4you.com

Plaintiffs' Co-Lead Interim Class Counsel

Gayle M. Blatt (*Pro Hac Vice*)
P. Camille Guerra (*Pro Hac Vice*)
CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
110 Laurel Street
San Diego, CA 92101
Tel.: 619.238.1811; Fax: 619.544.9232
gmb@cglaw.com
camille@cglaw.com

Gary M. Klinger (*Pro Hac Vice*)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: 866.252.0878
gklinger@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW, Suite 440
Washington, D.C. 20015-2052
Tel.: 866.252.0878; Fax: 202.686.2877
dlietz@milberg.com

**pro hac vice* application forthcoming

Attorneys for Plaintiffs and the putative Class

CERTIFICATE OF SERVICE

I hereby certify that on September 14, 2022, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP